

CLAIMS

- 1 1. A method for improving the security of a counter mode block cipher that breaks a
2 message into text bytes and encrypts each text byte with a fixed, secret key with
3 a keyszie, the method comprising:
4 (a) generating a random byte sequence for each message;
5 (b) combining the random byte sequence with the key to form a modified key;
6 and
7 (c) conveying the modified key to the block cipher so that each text byte is
8 encrypted with the modified key.
- 1 2. The method of claim 1 wherein the random byte sequence has same size as the
2 keyszie and step (b) comprises combining the random byte sequence with the
3 key with a bitwise exclusive-OR function.
- 1 3. The method of claim 1 wherein step (b) comprises concatenating the random
2 byte sequence with the key and passing the concatenation through a mask
3 generation function to obtain the modified key.
- 1 4. The method of claim 1 wherein the random byte sequence is non-secret.
- 1 5. The method of claim 1 wherein the mask generation function is a one-way
2 function.
- 1 6. Apparatus for improving the security of a counter mode block cipher that breaks
2 a message into text bytes and uses an encryption algorithm to encrypt each text
3 byte with a fixed, secret key with a keyszie, the apparatus comprising:
4 a sequence generator that generates a random byte sequence for each
5 message;

6 a key generator that combines the random byte sequence with the key to
7 form a modified key; and

8 a mechanism that conveys the modified key to the encryption algorithm so
9 that each text byte is encrypted with the modified key.

1 7. The apparatus of claim 6 wherein the random byte sequence has same size as
2 the keysize and the key generator comprises a bitwise exclusive-OR function that
3 combines the random byte sequence with the key.

1 8. The apparatus of claim 6 wherein the key generator comprises a mechanism that
2 concatenates the random byte sequence with the key and a mask generation
3 function that operates on the concatenation to obtain the modified key.

1 9. The apparatus of claim 6 wherein the random byte sequence is non-secret.

1 10. The apparatus of claim 6 wherein the mask generation function is a one-way
2 function.

1 11. A method for improving the security of a stream cipher that encrypts a continuous
2 byte stream of messages with a fixed, secret key with a keysizes, the method
3 comprising:

- 4 (a) generating a random byte sequence for each message;
- 5 (b) combining the random byte sequence with the key to form a modified key;
6 and
- 7 (c) conveying the modified key to the stream cipher so that each message
8 stream is encrypted with the modified key.

1 12. The method of claim 11 wherein the random byte sequence has same size as
2 the keysizes and step (b) comprises combining the random byte sequence with
3 the key with a bitwise exclusive-OR function.

- 1 13. The method of claim 11 wherein step (b) comprises concatenating the random
2 byte sequence with the key and passing the concatenation through a mask
3 generation function to obtain the modified key.
- 1 14. The method of claim 11 wherein the random byte sequence is non-secret.
- 1 15. The method of claim 11 wherein the mask generation function is a one-way
2 function.
- 1 16. Apparatus for improving the security of a stream cipher that encrypts a
2 continuous byte stream of messages with a fixed, secret key with a keyszie, the
3 apparatus comprising:
4 a sequence generator that generates a random byte sequence for each
5 message;
6 a key generator that combines the random byte sequence with the key to
7 form a modified key; and
8 a mechanism that conveys the modified key to the encryption algorithm so
9 that each message stream is encrypted with the modified key.
- 1 17. The apparatus of claim 16 wherein the random byte sequence has same size as
2 the keyszie and the key generator comprises a bitwise exclusive-OR function that
3 combines the random byte sequence with the key.
- 1 18. The apparatus of claim 16 wherein the key generator comprises a mechanism
2 that concatenates the random byte sequence with the key and a mask
3 generation function that operates on the concatenation to obtain the modified
4 key.
- 1 19. The apparatus of claim 16 wherein the random byte sequence is non-secret.

- 1 20. The apparatus of claim 16 wherein the mask generation function is a one-way
2 function.
- 1 21. A computer program product for improving the security of a stream cipher that
2 encrypts a continuous byte stream of messages with a fixed, secret key with a
3 keysizes, the computer program product comprising a computer usable medium
4 having computer readable code thereon, including:
5 program code that generates a random byte sequence for each message;
6 program code that combines the random byte sequence with the key to
7 form a modified key; and
8 program code that conveys the modified key to the stream cipher so that
9 each message stream is encrypted with the modified key.
- 1 22. The computer program product of claim 21 wherein the random byte sequence
2 has same size as the keysizes and the program code that generates a random
3 byte sequence comprises program code that combines the random byte
4 sequence with the key with a bitwise exclusive-OR function.
- 1 23. The computer program product of claim 21 wherein the program code that
2 generates a random byte sequence comprises program code that concatenates
3 the random byte sequence with the key and passes the concatenation through a
4 mask generation function to obtain the modified key.
- 1 24. The computer program product of claim 21 wherein the random byte sequence is
2 non-secret.
- 1 25. The computer program product of claim 21 wherein the mask generation function
2 is a one-way function.

- 1 26. A computer program product for improving the security of a counter mode block
2 cipher that breaks a message into text bytes and uses an encryption algorithm to
3 encrypt each text byte with a fixed, secret key with a keyszie, the computer
4 program product comprising a computer usable medium having computer
5 readable code thereon, including:
6 program code that generates a random byte sequence for each message;
7 program code that combines the random byte sequence with the key to
8 form a modified key; and
9 program code that conveys the modified key to the block cipher so that
10 each text byte is encrypted with the modified key.
- 0 1 27. The computer program product of claim 26 wherein the random byte sequence
2 has same size as the keyszie and the program code that generates a random
3 byte sequence comprises program code that combines the random byte
4 sequence with the key with a bitwise exclusive-OR function.
- 1 1 28. The computer program product of claim 26 wherein the program code that
2 generates a random byte sequence comprises program code that concatenates
3 the random byte sequence with the key and passes the concatenation through a
4 mask generation function to obtain the modified key.
- 1 29. The computer program product of claim 26 wherein the random byte sequence is
2 non-secret.
- 1 30. The computer program product of claim 26 wherein the mask generation function
2 is a one-way function.

- 1 31. A computer data signal embodied in a carrier wave for improving the security of a
2 stream cipher that encrypts a continuous byte stream of messages with a fixed,
3 secret key with a keys size, the computer data signal comprising:
4 program code that generates a random byte sequence for each message;
5 program code that combines the random byte sequence with the key to
6 form a modified key; and
7 program code that conveys the modified key to the stream cipher so that
8 each message stream is encrypted with the modified key.
- 1 32. A computer data signal for improving the security of a counter mode block cipher
2 that breaks a message into text bytes and uses an encryption algorithm to
3 encrypt each text byte with a fixed, secret key with a keys size, the computer data
4 signal comprising:
5 program code that generates a random byte sequence for each message;
6 program code that combines the random byte sequence with the key to
7 form a modified key; and
8 program code that conveys the modified key to the block cipher so that
9 each text byte is encrypted with the modified key.